H-VPLS N-PE Redundancy for QinQ Access

The H-VPLS N-PE Redundancy for QinQ Access feature enables two network provider edge (N-PE) devices to provide failover services to a user provider edge (U-PE) device in a hierarchical virtual private LAN service (H-VPLS). Having redundant N-PE devices provides improved stability and reliability against link and node failures.

- Finding Feature Information, page 1
- Prerequisites for H-VPLS N-PE Redundancy for QinQ Access, page 1
- Restrictions for H-VPLS N-PE Redundancy for QinQ Access, page 2
- Information About H-VPLS N-PE Redundancy for QinQ Access, page 2
- How to Configure H-VPLS N-PE Redundancy for QinQ Access, page 3
- Configuration Examples for H-VPLS N-PE Redundancy for QinQ Access, page 7
- Additional References, page 8
- Feature Information for H-VPLS N-PE Redundancy for QinQ Access, page 9
- Glossary, page 10

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for H-VPLS N-PE Redundancy for QinQ Access

- Before configuring this feature, configure your hierarchical virtual private LAN service (H-VPLS) network and make sure it is operating correctly.

- Make sure that the PE-to-customer edge (CE) interface is configured with a list of allowed VLANs.
- To provide faster convergence, you can enable the MPLS Traffic Engineering**—**Fast Reroute feature in the Multiprotocol Label Switching (MPLS) core.
- Enable the L2VPN Pseudowire Redundancy feature on the user provider edge (U-PE) devices for MPLS access.
- When configuring Multiple Spanning Tree Protocol (MSTP), specify that one of the network provider edge (N-PE) devices is the root by assigning it the lowest priority using the **spanning-tree mst** *instance-id* **priority** *priority* command.
- When configuring MSTP, make sure that each device participating in the spanning tree is in the same region and is the same revision by issuing the **revision**, **name**, and **instance** commands in MST configuration mode.

Restrictions for H-VPLS N-PE Redundancy for QinQ Access

- This feature cannot be used with the VPLS Autodiscovery feature on pseudowires that attach to network provider edge (N-PE) devices. When you create the virtual private LAN service (VPLS), you can manually create the virtual forwarding instance (VFI).
- You cannot configure more than one pseudowire to carry the bridge protocol data unit (BPDU) packets between two redundant network provider edge (N-PE) devices on the same Virtual Private LAN service (VPLS) site.
- You cannot configure a local loopback address as a neighbor when you configure the H-VPLS N-PE Redundancy feature on N-PE devices. If you do so, the following error message is displayed:

```
VPLS local switching to peer address not supported
```

- Only two N-PE devices can be connected to each U-PE device.
- The spanning-tree mode must be Multiple Spanning Tree Protocol (MSTP) for the H-VPLS N-PE Redundancy feature. If the spanning-tree mode changes, the H-VPLS N-PE Redundancy feature might not work correctly, even though the pseudowire that carries the BPDU packet still exists and the H-VPLS N-PE Redundancy feature is still configured.

Information About H-VPLS N-PE Redundancy for QinQ Access

How H-VPLS N-PE Redundancy for QinQ Access Works

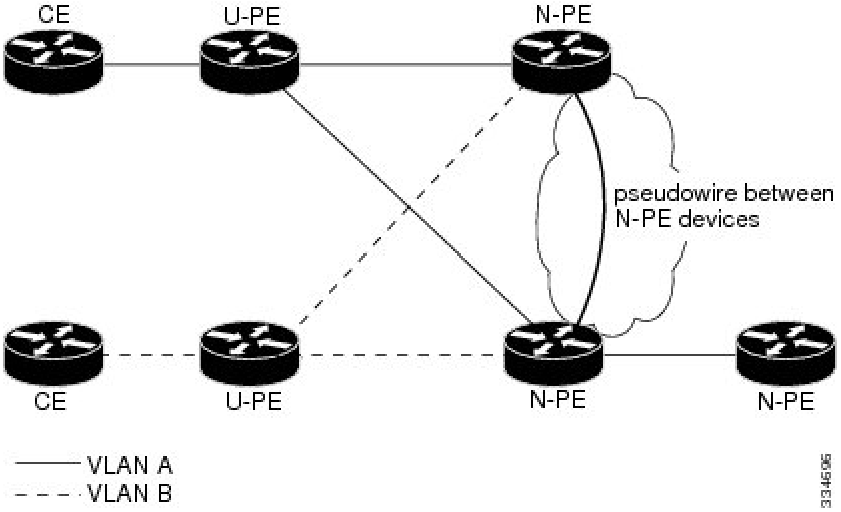
In a network configured with the H-VPLS N-PE Redundancy feature, the user provider edge (U-PE) device is connected to two network provider edge (N-PE) devices. This feature provides a level of redundancy that can tolerate both link and device faults. If a failure occurs in the network that disables one N-PE device from transmitting data, the other N-PE device takes over. This feature works with both QinQ access based on Multiple Spanning Tree Protocol (MSTP) and Multiprotocol Label Switching (MPLS) access based on pseudowire redundancy.

H-VPLS N-PE Redundancy with QinQ Access Based on MSTP

The H-VPLS N-PE Redundancy with QinQ Access feature uses the Multiple Spanning Tree Protocol (MSTP) running on the network provider edge (N-PE) devices and user provider edge (U-PE) devices in a hierarchical Virtual Private LAN service (H-VPLS) network. A pseudowire running between N-PE devices carries only MSTP bridge protocol data units (BPDUs). The pseudowire running between the N-PE devices is always up and is used to create a loop path between N-PE devices so that MSTP blocks one of the redundant paths between the U-PE device and the N-PE devices. If the primary N-PE device or the path to it fails, MSTP enables the path to the backup N-PE device.

The figure below shows an H-VPLS network with redundant access. Each U-PE device has two connections, one to each N-PE device. Between the two N-PE devices is a pseudowire to provide a loop path for MSTP BPDUs. The network topology allows for the backup N-PE device to take over if the primary N-PE device or the path to it fails.

Figure 1: H-VPLS N-PE Redundancy with QinQ Access Based on MSTP



How to Configure H-VPLS N-PE Redundancy for QinQ Access

Configuring the VPLS Pseudowire Between the N-PE Devices

Configuring network provider edge (N-PE) redundancy in a hierarchical Virtual Private LAN service (H-VPLS) network requires that you define the VPLS pseudowire for transporting bridge protocol data unit (BPDU) packets (described here) and that you connect that pseudowire to the native VLAN (described in the next task). This configuration provides a redundancy that provides improved reliability against link and node failures.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **l2 vfi** *name* **manual**
4. **vpn id** *id-number*
5. **forward permit l2protocol all**
6. **neighbor** *remote-router-id vc-id* {**encapsulation** *encapsulation-type* | **pw-class** *pw-name*} [**no-split-horizon**]
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**l2 vfi** *name* **manual** **Example:** `Device(config)# l2 vfi vfitest1 manual`	Creates a Layer 2 virtual forwarding interface (VFI) and enters Layer 2 VFI manual configuration mode.
Step 4	**vpn id** *id-number* **Example:** `Device(config-vfi)# vpn id 200`	Specifies the VPN ID.
Step 5	**forward permit l2protocol all** **Example:** `Device(config-vfi)# forward permit l2protocol all`	Creates a pseudowire that is to be used to transport BPDU packets between the two N-PE devices.

	Command or Action	Purpose
Step 6	**neighbor** *remote-router-id vc-id* {**encapsulation** *encapsulation-type* | **pw-class** *pw-name*} [**no-split-horizon**] **Example:** `Device(config-vfi)# neighbor 10.2.2.2 3 encapsulation mpls`	Specifies the peer IP address of the redundant N-PE device and the type of tunnel signaling and encapsulation mechanism.

Step 7	**end**
	Example:
	`Device(config-vfi)# end`
		Exits Layer 2 VFI manual configuration mode and returns to privileged EXEC mode.

Configuring the SVI for the Native VLAN

Perform this task to configure the switched virtual interface (SVI) for the native VLAN and verify that it is correctly configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vlan** *vlan-id*
4. **xconnect vfi** *vfi-name*
5. **end**
6. **show vfi** *vfi-name*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 23`	Creates a dynamic SVI. • To make the SVI active when you create a VLAN, you must configure the VLAN with at least one physical interface that is in the “up” state. Use the **show vfi** command to display the status of the SVI. The state field will display “up” when the SVI is active.
Step 4	**xconnect vfi** *vfi-name* **Example:** `Device(config)# xconnect vfi vfitest1`	Specifies the Layer 2 virtual forwarding interface (VFI) that you are binding to the VLAN port.

Step 5	**end**
	Example:
	`Device(config-vfi)# end`
		Ends the current configuration session and returns to privileged EXEC mode.

Step 6	**show vfi** *vfi-name* **Example:** `Device# show vfi VPLS-2`	(Optional) Displays information about the pseudowire between the two network provider edge (N-PE) devices so that you can verify that the H-VPLS N-PE Redundancy feature is correctly configured.

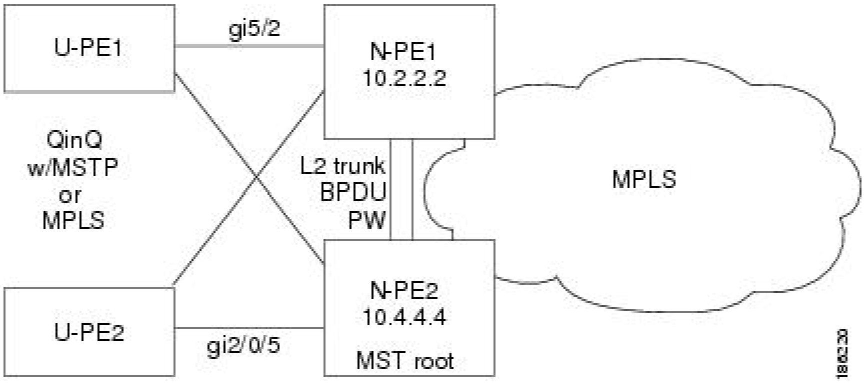
Step 7	**end**
	Example:
	`Device# end`
		Exits privileged EXEC mode and returns to user EXEC mode.

Configuration Examples for H-VPLS N-PE Redundancy for QinQ Access

Example: H-VPLS N-PE Redundancy for QinQ Access

The figure below shows a configuration that is set up for the H-VPLS N-PE Redundancy with QinQ Access feature.

Figure 2: H-VPLS N-PE Redundancy with QinQ Access Topology



The table below shows the configuration of two network provider edge (N-PE) devices.

Table 1: Example: H-VPLS N-PE Redundancy for QinQ Access

N-PE1	N-PE2

`l2 vfi l2trunk manual`
` vpn id 10`
` forward permit l2protocol all`
` neighbor 10.4.4.4 encapsulation mpls`
`!`
`interface Vlan1`
` no ip address`
` xconnect vfi l2trunk`
`!`
`spanning-tree mode mst`
`spanning-tree extend system-id`
`!`
`spanning-tree mst configuration`
` revision 10`
` instance 1 vlan 20`
`!`
`interface GigabitEthernet5/2`
` switchport`
` switchport trunk encapsulation dot1q`
` switchport trunk allowed vlan 20`
` switchport mode trunk`
	`l2 vfi l2trunk manual`
	` vpn id 10`
	` forward permit l2protocol all`
	` neighbor 10.2.2.2 encapsulation mpls`
	`!`
	`interface Vlan1`
	` no ip address`
	` xconnect vfi l2trunk`
	`!`
	`spanning-tree mode mst`
	`spanning-tree extend system-id`
	`!`
	`spanning-tree mst configuration`
	` revision 10`
	` instance 1 vlan 20`
	`!`
	`spanning-tree mst 1 priority 0`
	`!`
	`interface GigabitEthernet2/0/5`
	` switchport`
	` switchport trunk allowed vlan 20`
	` switchport mode trunk`
	` mls qos trust dscp`

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
MPLS commands	Cisco IOS Multiprotocol Label Switching Command Reference
L2VPN pseudowire redundancy	“L2VPN Pseudowire Redundancy” feature module in the *MPLS Layer 2 VPNs Configuration Guide*.
H-VPLS	“Configuring VPLS” in the “Configuring Multiprotocol Label Switching on the Optical Services Modules” chapter in the *Optical Services Modules Installation and Configuration Notes*, 12.2SR document.
MPLS traffic engineering	“MPLS Traffic Engineering Fast Reroute Link and Node Protection” feature module in the *MPLS Traffic Engineering: Path, Link, and Node Protection Configuration Guide* (part of the Multiprotocol Label Switching Configuration Guide Library)

Standards

Standard	Title
http://www.ietf.org/rfc/rfc4447.txt	*Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*
http://www3.ietf.org/proceedings/06mar/IDs/draft-ietf-l2vpn-vpls-ldp-08.txt	*Virtual Private LAN Services over MPLS*
http://www.ietf.org/internet-drafts/draft-ietf-pwe3-segmented-pw-02.txt	*Segmented Pseudo Wire*
draft-ietf-pwe3-vccv-10.txt	*Pseudo Wire Virtual Circuit Connectivity Verification (VCCV)*
draft-ietf-pwe3-oam-msg-map-03.txt	*Pseudo Wire (PW) OAM Message Mapping*

MIBs

MIB	MIBs Link
Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for H-VPLS N-PE Redundancy for QinQ Access

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for H-VPLS N-PE Redundancy for QinQ Access

Feature Name	Releases	Feature Information
H-VPLS N-PE Redundancy for QinQ Access	12.2(33)SRC 12.2(50)SY Cisco IOS XE Release 3.8S	The H-VPLS N-PE Redundancy for QinQ Access feature provides the capability to dual-home a given user provider edge (U-PE) device to two network provide edge (N-PE) devices in order to provide protection against link and node failures. In Cisco IOS Release 12.2(33)SRC, this feature was introduced on the Cisco 7600 series routers. In Cisco IOS Release 12.2(50)SY, this feature was integrated. In Cisco IOS XE Release 3.8S, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **forward permit l2protocol**, **show mpls l2transport vc**.

Glossary

CE device—customer edge device. A device that belongs to a customer network, which connects to a PE device to utilize MPLS VPN network services.

LAN—local-area network. High-speed, low-error data network covering a relatively small geographic area. LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited areas.

MPLS—Multiprotocol Label Switching. A packet-forwarding technology, used in the network core, that applies data link layer labels to tell switching nodes how to forward data, resulting in faster and more scalable forwarding than network layer routing normally can do.

MSTP—Multiple Spanning Tree Protocol. MSTP enables multiple VLANs to be mapped to the same spanning-tree instance, reducing the number of spanning-tree instances needed to support a large number of VLANs.

N-PE—network provider edge device. This device acts as a gateway between the MPLS core and edge domains.

PE device—provider edge device. The PE device is the entry point into the service provider network. The PE device is typically deployed on the edge of the network and is administered by the service provider.

pseudowire—A pseudowire is a virtual connection that, in the context of VPLS, connects two SVIs. It is a mechanism that carries the elements of an emulated service from one PE device to one or more PE devices over a packet switched network (PSN). A pseudowire is bidirectional and consists of a pair of unidirectional MPLS virtual circuits (VCs). A pseudowire can be used to connect a point-to-point circuit.

QinQ—An IEEE 802.1Q VLAN tunnel. A mechanism for constructing multipoint Layer 2 VPN using Ethernet switches.

redundancy—The duplication of devices, services, or connections so that, in the event of a failure, they can perform the work of those that failed.

router—A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

spanning tree—Loop-free subset of a network topology.

U-PE—user provider edge device. This device connects CE devices to the service.

VFI—virtual forwarding instance. A VFI is a collection of data structures used by the data plane, software-based or hardware-based, to forward packets to one or more VCs.

VLAN—Virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments.

VPLS—Virtual Private LAN Service. VPLS describes an architecture that delivers Layer 2 service that emulates an Ethernet LAN across a wide-area network (WAN) and inherits the scaling characteristics of a LAN.

VPLS redundancy—Also called N-PE redundancy. Allows U-PEs to be dual-honed (to their N-PEs) in a loop-free topology with MPLS or QinQ as the access or aggregation domain.

VPN—Virtual Private Network. Allows IP traffic to travel securely over public TCP/IP networks and the Internet by encapsulating and encrypting all IP packets. VPN uses a tunnel to encrypt all information at the IP level.